Translation

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference 10028	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/JP2003/007794	International filing date (*day/month/year*) 19 June 2003 (19.06.2003)	Priority date (*day/month/year*) 19 June 2002 (19.06.2002)
International Patent Classification (IPC) or national classification and IPC H04L 9/32		
Applicant ADVANCED COMPUTER SYSTEMS, INC.		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 15 sheets, including this cover sheet.

   ☒ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of 2 sheets.

3. This report contains indications relating to the following items:

   - I ☒ Basis of the report
   - II ☐ Priority
   - III ☒ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - IV ☒ Lack of unity of invention
   - V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
   - VI ☐ Certain documents cited
   - VII ☐ Certain defects in the international application
   - VIII ☒ Certain observations on the international application

Date of submission of the demand 19 June 2003 (19.06.2003)	Date of completion of this report 19 February 2004 (19.02.2004)
Name and mailing address of the IPEA/JP Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/JP2003/007794

I. Basis of the report

1. With regard to the **elements** of the international application:*

☐ the international application as originally filed

☒ the description:

pages 1-36, 38-70, as originally filed
pages _____, filed with the demand
pages 37, filed with the letter of 09 February 2004 (09.02.2004)

☒ the claims:

pages 1-26, 28-50, as originally filed
pages _____, as amended (together with any statement under Article 19
pages _____, filed with the demand
pages 27, filed with the letter of 09 February 2004 (09.02.2004)

☒ the drawings:

pages 1-16, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____

☐ the sequence listing part of the description:

pages _____, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.
These elements were available or furnished to this Authority in the following language _____ which is:

☐ the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).

☐ the language of publication of the international application (under Rule 48.3(b)).

☐ the language of the translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

☐ contained in the international application in written form.

☐ filed together with the international application in computer readable form.

☐ furnished subsequently to this Authority in written form.

☐ furnished subsequently to this Authority in computer readable form.

☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☐ The amendments have resulted in the cancellation of:

☐ the description, pages _____

☐ the claims, Nos. _____

☐ the drawings, sheets/fig _____

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).**

* *Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rule 70.16 and 70.17).*

** *Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.*

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/JP2003/007794

III. Non-establishment of opinion with regard to novelty, inventive step and industrial applicability

1. The questions whether the claimed invention appears to be novel, to involve an inventive step (to be non obvious), or to be industrially applicable have not been examined in respect of:

☐ the entire international application.

☒ claims Nos. 1-13, 27

because:

☐ the said international application, or the said claims Nos. _____ relate to the following subject matter which does not require an international preliminary examination *(specify)*:

☒ the description, claims or drawings *(indicate particular elements below)* or said claims Nos. 1-13 are so unclear that no meaningful opinion could be formed *(specify)*:

See supplemental sheet

☐ the claims, or said claims Nos. _____ are so inadequately supported by the description that no meaningful opinion could be formed.

☒ no international search report has been established for said claims Nos. 1-13, 27 .

2. A meaningful international preliminary examination cannot be carried out due to the failure of the nucleotide and/or amino acid sequence listing to comply with the standard provided for in Annex C of the Administrative Instructions:

☐ the written form has not been furnished or does not comply with the standard.

☐ the computer readable form has not been furnished or does not comply with the standard.

Supplemental Box
(To be used when the space in any of the preceding boxes is not sufficient)

Continuation of: III. 1.

It is unclear whether the phrase "the newly generated stored data" in the portion of claim 1 stating that "the newly generated stored data is encrypted using the aforementioned historical data and transmitted to a second authentication device" refers to the same data as the phrase "stored data" in the portion stating that "the aforementioned first authentication device generates new stored data using the stored historical data." Similarly, it is also unclear whether the phrase "the newly generated stored data" in the portion stating that "the newly generated stored data is encrypted using the aforementioned historical data and transmitted to a first authentication device" refers to the same data as the phrase "stored data" in the portion stating that "the aforementioned second authentication device... generates new stored data using the stored historical data." Further, if each phrase refers to different data, the significance of generating stored data using historical data is unclear. In the same manner, it is unclear whether the phrase "stored data from the first authentication device" in the portion stating that "the aforementioned second authentication device generates new stored data using... stored data from the first authentication device" refers to the same data as the phrase "stored data" in the specification of "a first transmitting procedure wherein the newly generated data... is encrypted and transmitted to a second authentication device," and if the phrases refer to different data, it is unclear what kind of data the "stored data from the first authentication device" is.

Supplemental Box
(To be used when the space in any of the preceding boxes is not sufficient)

Continuation of: III. 1.

Furthermore, claim 1 includes portions stating that "the aforementioned first authentication device generates new stored data using the stored historical data" and that "the aforementioned second authentication device... generates new stored data using the stored historical data," but it is unclear whether the phrase "historical data" refers to the same data indicated by the phrase "historical data" in the portion stating that "update results of an update performed using the stored data from the previous authentication [is stored] as historical data," and if the phrases refer to different data, it is unclear what kind of data are indicated by the phrase "historical data" and the later phrase "aforementioned historical data."

Moreover, it is also unclear what kind of data is indicated by the phrase "stored data from the previous authentication" in the portion stating that "update results of an update performed using the stored data from the previous authentication [is stored] as historical data."

Thus, it cannot be ascertained by what sequence of procedures authentication is carried out in the "mutual authentication method" described in claim 1 because the relationship between the plurality of "stored data" and "historical data" is unclear. The same applies to claims 2 to 13, which refer back to claim 1.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/JP2003/007794

IV. Lack of unity of invention

1. In response to the invitation to restrict or pay additional fees the applicant has:

☐ restricted the claims.

☐ paid additional fees.

☐ paid additional fees under protest.

☐ neither restricted nor paid additional fees.

2. ☒ This Authority found that the requirement of unity of invention is not complied with and chose, according to Rule 68.1, not to invite the applicant to restrict or pay additional fees.

3. This Authority considers that the requirement of unity of invention in accordance with Rules 13.1, 13.2 and 13.3 is

☐ complied with.

☒ not complied with for the following reasons:

See supplemental sheet

4. Consequently, the following parts of the international application were the subject of international preliminary examination in establishing this report:

☐ all parts.

☒ the parts relating to claims Nos. 14-26, 28-50 .

Supplemental Box
(To be used when the space in any of the preceding boxes is not sufficient)

Continuation of: IV. 3.

Claims 1 to 13 describe an invention pertaining to mutual authentication that has no relationship to a one-time ID. Claims 14 to 50 describe an invention pertaining to a one-time ID. Furthermore, mutual authentication is known in the art, and thus, mutual authentication cannot be used as a "special technical feature."

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/JP 03/07794

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	14, 15, 17, 18, 20-24, 26, 28-43, 47-50	YES
	Claims	16, 19, 25, 44-46	NO
Inventive step (IS)	Claims	14, 15, 17, 18, 20-24, 26, 28-43, 47-50	YES
	Claims	16, 19, 25, 44-46	NO
Industrial applicability (IA)	Claims	14-26, 28-50	YES
	Claims		NO

2. Citations and explanations

Claims 16, 19, and 44 to 46 lack novelty in the light of document 1 (*Handbook of Applied Cryptography*, CRC Press, 1997, pages 400-403) cited in the international search report. Document 1 discloses an invention pertaining to "an authentication method wherein
B transmits a challenge r_B to *A*, and
A calculates the unidirectional function value $h_K(\ldots r_B \ldots)$ using the above challenge r_B and a shared key *K* as arguments, and transmits this unidirectional function value $h_K(\ldots r_B \ldots)$ and a challenge r_A to *B*, and
B calculates the unidirectional function value $h_K(\ldots r_B \ldots)$ using the above challenge r_B and the shared key *K* as arguments, and compares this value and the unidirectional function value $h_K(\ldots r_B \ldots)$ received from *A* to determine the authenticity of *A*, and
B calculates the unidirectional function value $h_K(r_B, r_A \ldots)$ using the above challenges r_A and r_B and the shared key *K* as arguments, and transmits this value to *A*, and
A calculates the unidirectional function value $h_K(r_B, r_A \ldots)$ using the above challenges r_A and r_B and the shared key *K* as arguments, and compares this value and the unidirectional function value $h_K(r_B, r_A \ldots)$ received from *B* to determine the authenticity of *B*."

It is known as a matter of course in this technical field that a challenge is a random number newly generated for each challenge, and thus, the unidirectional function values are also data limited to one-time use. Further, as noted in Box VIII, the "one-time ID" described in these claims is not recognized as an "ID" in the sense in which the term is generally used, but rather, is data for use in determining the authenticity of an entity, and thus, no significant difference is found between the unidirectional function value in the invention disclosed in document 1 and the "one-time ID" described in these claims. Moreover, as also noted in Box VIII, the significance of generating and transmitting "a first one-time ID" is unclear, and thus, no particular significance is recognized in the presence of said procedure.

Claims 14, 15, 17, 18, 20 to 24, 26, 28 to 43, and 47 to 50 are novel and involve an inventive step. The inventions described in these claims are neither disclosed nor suggested in the documents.

VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

(a) The invention described as embodiment 1 in the description and drawings could be forged by a third party, and does not substantially function to provide authentication, as explained below.

The relationships between data transmitted between a client and a server are as expressed below.

$$S_{m+1} = C_{m+1} + Q_m,\ C_{m+1} = S_m + R_m,\ A_m = R_m + K_{m-1},\ B_m = Q_m + K_{m-1}$$

The following two expressions are derived from these four relational expressions.

$$S_{m+1} - S_m = Q_m + R_m,\ A_m - B_m = Q_m + R_m$$

Therefore, Q_m and R_m can be calculated using the following equations.

$$Q_m = (S_{m+1} - S_m - A_m + B_m)/2,\ R_m = (S_{m+1} - S_m + A_m - B_m)/2$$

Here, S_{m+1}, S_m, A_m, and B_m all refer to data appearing along a transmission pathway between a client and a server, and thus, a third party could intercept these data and use them to determine Q_m and R_m. Further, C_m and S_m also appear along a transmission pathway, and thus, a third party could use Q_m, R_m, C_m, and S_m to determine K_m. Therefore, Q_{m+1} and R_{m+1} can be calculated using the following equations.

$$Q_{m+1} = B_{m+1} - K_m,\ R_{m+1} = A_{m+1} - K_m$$

VIII. Certain observations on the international application

K_{m+1} can also be determined using the above Q_{m+1} and R_{m+1} together with C_{m+1} and S_{m+1}, which appear along a transmission pathway. That is to say, any given private key can be calculated simply by observing data appearing along a transmission pathway. This means that any given third party could pass itself off as either a client or server, and thus, the invention described as embodiment 1 does not substantially provide mutual authentication.

(b) The description of step S2 in embodiment 2 indicates that a server determines a SIGNAL by performing a computation. Here, a key K_{i-1} is required for the computation of $SIGNAL_i$, and the three elements of a given server/client shared key, a DH shared key g^{xy}, and $SIGNAL_{i-1}$ are required in order to perform the computation of the key K_{i-1}. However, while a review of the description does indicate that the DH shared key g^{xy} is stored in a memory device (13), there is no particular indication that the $SIGNAL_{i-1}$ is stored, and thus it is unclear how the $SIGNAL_{i-1}$ is obtained. Moreover, even assuming that the $SIGNAL_{i-1}$ is stored in the memory device, the following aspect of the use of the DH shared key g^{xy} and the $SIGNAL_{i-1}$ is unclear. Namely, in general, a server has a plurality of clients connected thereto, and in such a case, it is recognized that the DH shared key g^{xy} and the $SIGNAL_{i-1}$ differ for each client. This being the case, when the server uses these data, the server must select from among the plurality of pairs of data corresponding to the plurality of clients in order to find the data corresponding to the client requesting connection. However, the $SIGNAL_i$

VIII. Certain observations on the international application

transmitted from a client is data that changes with each connection, and thus, said data cannot be used to specify the client. Accordingly, it is unclear how the server selects the data required in order to calculate the key K_{i-1} and, by the same token, the $SIGNAL_i$.

Meanwhile, this means that, depending on the SIGNAL received, a server cannot "specify," or more particularly, "identify" the corresponding client. Further, in step S2, the authenticity of a client is determined by performing a comparison using the SIGNAL, but this would mean that although the SIGNAL cannot be used in order to identify "which client is requesting connection," it is used in order to determine "whether the client requesting connection is legitimate." That is to say, the SIGNAL functions more as a "password" than as an "ID."

Further, a client uses a server's SIGNAL when determining the authenticity of the server, but the client can be said to have "identified" said server at the time when it transmitted a connection request to the server, and thus, the indication that a server's SIGNAL is that server's "ID" or, more particularly, "identifying data" is unclear.

Consequently, the indication that these SIGNALs are the "IDs" or, more particularly, the "identifying data" for a client or a server is unclear, and thus, the indication in the description that these SIGNALs are "one-time IDs" or, more particularly, "identifying data that can be used only one time" is unclear.

VIII. Certain observations on the international application

(c) The description of step P2 in embodiment 3 indicates that a server determines a SIGNAL by performing a computation, which it then compares with a received SIGNAL in order to "identify" a client. However, as stated in item (b), data corresponding to a client is required in order to perform the SIGNAL computation, and thus, a client must already by "specified" or more particularly, "identified" at the time of this computation. This being the case, the significance of a client being "identified" by a comparison of a computed SIGNAL and a received SIGNAL is unclear. Further, if this "identification" by comparison is not an identification of "what client is requesting connection," but rather an identification of "whether the party requesting connection is a valid client," the description, as stated above in item (b), should indicate that the SIGNAL is data corresponding more to a "password" than to an "ID," and thus, the description of said SIGNAL as a "one-time ID" is unclear. The same thing can be said about the "identification" of a server by a client, and as stated above in item (b), a client can be said to have "identified" a server at the time it transmitted a connection request to said server, and thus, it is also unclear why the SIGNAL a server transmits to a client is described as a "one-time ID."

The same applies to embodiments 4, 5, 6, and 7.

(d) The description of embodiment 8 indicates that steps S61 and 62 can be skipped when a session number n is stored in a client. However, if these steps are skipped, the server is not notified of the client's

VIII. Certain observations on the international application

ID_c, and thus, when calculating the SIGNAL, it is unclear how the server selects authentication data corresponding to the client. Consequently, the description of the SIGNAL as a "one-time ID" is unclear, as stated in items (b) and (c).

(e) As stated above, in the inventions described as embodiments 2 to 8, a receiving side cannot "identify" a transmitting side using a SIGNAL, and the description only indicates that a receiving side uses the SIGNAL in the manner of a password when "validated" by the transmitting side, and thus, it is recognized that in the "identification" of the transmitting side, data other than the SIGNAL and which is not disclosed in the description is required. Accordingly, the description of the present application is not recognized as providing sufficient support for the features described in claims 14 to 50.

(f) The description of embodiment 4 indicates that a client calculates a $SIGNAL_{C1}$, which it then transmits to a server, but there is no description of any process carried out by the server using this $SIGNAL_{C1}$. Thus, the significance of the client calculating a $SIGNAL_{C1}$ and transmitting it to a server is unclear. The same applies to embodiment 5.

(g) The description of embodiment 5 calls the $SIGNAL_{C1}$ transmitted by a client to a server a "one-time ID." However, the shared key K used in the calculation of the $SIGNAL_{C1}$ is fixed and does not change, nor is there any description of updating and changing a

VIII. Certain observations on the international application

random number R_0, and thus, the $SIGNAL_{C1}$ is not recognized as data that changes with each transmission, and this is another reason the description of $SIGNAL_{C1}$ as a "one-time ID" is unclear. Accordingly, it is also for this reason that the description of the present application is not recognized as providing sufficient support for the features described in claims 16, 19, 25, 44, 45, and 46.